§ 12. Показател на число по даден модул

Нека ** е естествено число и *a* е цяло число, взаимно просто с *n*. От теоремата на Ойлер знаем, че . Най-малкото естествено число *r* със свойството  се нарича *показател на a по модул n*. Ще казваме още, че *a принадлежи на показател r по модул n.* По-нататък, като говорим за показател на число по даден модул, винаги ще имаме предвид, че това число е взаимно просто с модула.

**Твърдение 12.1.** *Ако a принадлежи на показател r по модул n, числата  са несравними по модул n.*

*Доказателство.* Да допуснем, че  и . Тогава числото *n* дели разликата . Тъй като , то , т.е. . Но това противоречи на определението за показател, защото .

**Твърдение 12.2 (основно свойство на показателя).** *Нека a принадлежи на показател r по модул n и . Тогава  точно когато .*

*Доказателство.* Да разделим *m* на *r* с частно и остатък:  . Тогава . Тъй като , то . Следователно  точно когато . Но от определението за показател следва, че последното е възможно единствено когато , т.е. когато .

**Следствие 12.3.** *Ако числото a принадлежи на показател r по модул n, то .*

**Упражнение 12.4.** *Да се докаже, че ако числото a принадлежи на показател r по модул n и , то числото  принадлежи на показател l по модул n.*

Това твърдение (освен че се проверява непосредствено) е частен случай от следващото твърдение.

**Твърдение 12.5.** *Нека числото a принадлежи на показател r по модул n и .Тогава числото  принадлежи на показател  по модул n. В частност, числото  принадлежи на същия показател r, както и числото a, точно когато .*

*Доказателство.* Нека  и ; тогава  Нека числото ** принадлежи на показател *t* по модул *n*. Искаме да покажем, че .

Имаме

.

Следователно . От друга страна, от



следва, че , т.е. че . Но  и значи . Окончателно получаваме, че .

**Твърдение 12.6.** *Нека числото a принадлежи на показател r по модул n, а числото b принадлежи на показател s по модул n. Тогава*

*а) ако , то числото  принадлежи на показател  по модул n;*

*б) съществува число c, чийто показател по модул n е равен на .*

*Доказателство.* *а)* Нека ** принадлежи на показател *t* по модул *n*. От  следва, че . От друга страна имаме , откъдето . Но , а значи и . Тогава  и от ** следва . По същия начин се получава, че . Тъй като **, то . Окончателно, .

*б)* Нека , където  са различни прости числа и  за . Тогава , където .

Съществува число , принадлежащо на показател  по модул *n*. Действително, ако числото  е равно (например) на , то числото *a*, повдигнато на степен  принадлежи на показател  по модул *n* (упражнение 12.4). Продължавайки по същия начин, се уверяваме, че съществува число , принадлежащо на показател  по модул *n*. Тъй като числата  са две по две взаимно прости, с неколкократно прилагане на подусловие а) заключаваме, че показателят на числото  по модул *n* е равен на **.